Security Issues in Near Field Communications (NFC)

Arwa Alrawais
College of Computer Engineering and Sciences
Prince Sattam Bin Abdulaziz University
Al-Kharj 11942, Saudi Arabia.

Abstract—**Near Field Communications (NFC) is a rising technology that enables two devices that are within close proximity to quickly establish wireless contactless communications. It looks intuitively secure enough and various applications like ticketing, mobile payments, access grant etc. are taking advantage of NFC and flooding into the market in recent years. However, is it worth to trust such applications at the risk of leaking the user's private information? This paper surveys NFC vulnerabilities and exploits different kinds of security attacks. Upon surveying related materials, the paper covered possible solutions that could defend against those security threats. Furthermore, attacks and countermeasures evaluation in terms of practicality and cost have been further investigated.**

Keywords*—*Near Field Communications (NFC); NFC attacks; NFC countermeasures; NFC vulnerabilities

I. Introduction

NFC (Near Field Communications) provides bidirectional, wireless, contactless communications for two NFC enabled devices or NFC tags within a short transmission range of less than 10 cm. It is derived from the Radio Frequency Identification technology, or RFID, whereas RFID is only capable of one-way transmission. NFC is based on inductive coupling to connect two NFC devices, or tags to establish communication at a central frequency of 13.56MHz, which is supported by ISO14443 standards.

NFC has three working modes, peer-to-peer mode, read/write mode, and NFC card emulation mode. The peer-to-peer working mode allows two NFC devices to transmit data between them. Read/write mode enables the NFC devices to access certain digital data. NFC card emulation mode, perhaps is the most interesting working mode, makes the NFC devices function as a NFC card. Based on activeness of the involved NFC devices or tags, the communication modes could be classified as active-active, active-inactive, inactive-active communication modes.

As an emerging technology, NFC has a promising and broad future to be applied in various kinds of applications. Currently, many key players of electronic communication market are involved in the NFC development [1], such as HP, Philips, Motorola, MasterCard, VISA, Panasonic, Microsoft, Gemalto, Vodafone, Siemens etc. NFC provides us with convenient tools like e-ticketing, electronic wallets, financial transactions, smart posters, etc. [2].

Among those wireless communications like WiFi, RFID, ZigBee and so on, why does electronic market favor NFC applications? NFC has the shortest transmission range and also the smallest data rate among the wireless communications. This means NFC has the advantage of quickly building a private communications within short distance. Table I shows that NFC is faster and easier to set up.

NFC appears to resist malicious attempts since they could only happen within a really short range. But is it safe enough for the users to rely on NFC applications instead of doing things in the conventional ways? The answer is negative. For one thing that NFC is a measure of wireless communication, which makes it vulnerable to eavesdropping, data corruption, and jamming attack. For another, NFC technology itself doesn't include strong security scheme to protect those applications that are built upon it. This leaves the job to the software designers and developers to seek ways to avoid any threats that could be caused by malfunction.

Though a NFC communication happens within close proximity, it doesn't mean that NFC is resistant to eavesdropping, jamming, data corruption, and other attacks towards wireless connection. Plus, NFC shares the basic standards and techniques with the proximity RFID technology. Some of the attacks that could be launched against RFID communications are major threats to NFC. How to defend against relay attack is an open problem in NFC communications, just like it's an unresolved problem in other wireless communications. Researches [4], [5], exploit the possibility of applying relay attack upon NFC communication. Imagine you have to use your NFC card to gain access to a building. What a malicious attacker could do is that he can attach a small receiver to the gate RF reader and record the signal sent by a legitimate NFC card. In this case, when a legitimate NFC card comes close to the reader, it thinks that it is sending signals to the reader. In fact, it is the "recorder" that is listening to the signal and tries to make a copy. Then the adversary could take advantage of this copy to do things like, clone a NFC card or use it to gain access.

As mentioned before, NFC doesn't provide any security mechanism to protect its communication, which leads to users' privacy being exposed to air. Even the Secure Element designed by Google to plot in a Google NFC device isn't secure as it sounds. The author in [6] addresses some issues when it comes to malware threats. The android operating system has proven to be vulnerable to malware attack, let alone the embedded SE, which is an obvious weak point when some malicious softwares try to gain information stored in SE through OS. For rooted devices, the SE access PIN is hashed using SHA256 and stored in the device rather than the SE. An attacker can brute-force the PIN and access the SE.

TABLE I. COMPARISON AMONG NFC, RFID, IRDA, BLUETOOTH [3]

	NFC	RFID	irDa	Bluetooth
Set -up time	¡ 0.1ms	¡ 0.1ms	˜ 0.5s	˜ 0.6s
Range	Up to 10cm	Up to 3m	Up to 5m	Up to 30m
Usability	Human centric Easy, intuitive, fast.	Item centric Easy	Data centric Easy	Data centric Easy
Selectivity	High given Security	Partly given	Line of sight	Who are you?
Use cases	Pay, get access, share, initiate service, easy set up	Item tracking	Control and exchange data	Network for data exchange, headset
Consumer experience	Touch, wave, simply connect	Get information	Easy	Configuration needed

The rest of this paper is organized as follows. In Section II, the paper summarize some related papers that talk about NFC technology and its vulnerabilities. In Section III, an illustration of the possible threats towards NFC technology and NFC applications along with the corresponding countermeasures to deal with these issues is introduced. At the end of Section III, an evaluation of the attacks and protection methods according is provided. At last, the author draw a conclusion of the study and point out some open problems about NFC in Section IV.

II. RELATED WORK

The growing number of released NFC applications raise concerns about its security issues. Lots of researchers have attempted to analyze the vulnerabilities of NFC technologies. The threats fall into two categories according to two characteristics the threats are aiming at, issues that intend to happen to wireless communications and dangers of malfunction of NFC applications or the operating system that carries the NFC softwares.

The authors in [6]–[10] make the point that eavesdropping attack is still possible in NFC connection. [7] claims that an antenna that is placed within distance of 10m can still "overhear" the data sent by an active NFC devices. This distance drops to 1m when the device is on passive working mode. Still, it makes eavesdropping possible. Thus, it opens the door for other threats like data corruption, data insertion, etc. Also, [7], [8] point out that using a RFID jammer or other devices that emit RF signals can easily jam or corrupt the data transmitted between two NFC devices. [9], [10] indicate that NFC is vulnerable to data modification attack, which is obvious since NFC doesn't encrypt the exchanged message. In addtion, [10] lists other potential attacks like data corruption, data insertion, and man in the middle attack. After trying to implement an secure offline payment application, Van Damme et al. [9] state that current technology is not sufficient to provide for a completely secured system not only because heavy use of cryptography will increase overhead, also because the hardware they used has limitations that slow down transaction speed and increase code complexity. In [11], the authors investigate man in the middle attack in NFC communications through performing a real time implementation in contactless payment system. They conduct man in the middle attack in NFC communications between passive tag and active terminal. Their results reported potential vulnerabilities in NFC communications due to the separation between payment card and point of sale.

In [4], [5], [12], the researchers claim that relay attack is also a big security concern in NFC. [12] even says that NFC is particularly vulnerable to relay attack and the authors provide countermeasures such as monitoring additional delay in propagation time, asking user to perform verification and integrating location information into transaction to protect NFC communication against relay attack. [4] points out that a malicious user could apply relay attack to gain access to Secure Element (SE) in a Google NFC device to pretend that he/she is in physical possession of the device. Michael Roland [4] mentions other malware threats about NFC devices. Both [5] and [4] talk about launching denial-of-service attack by simply touching a NFC devices using any arbitrary tags.

Upon cracking up the exchanged message between two NFC entities, [13] indicates that privacy infringement happens since NFC standards do not provide unlinkability between user message and public keys are constantly used in key agreements and the authors proposed a conditional anonymity using dynamic public key to solve this problem.

Collin Mulliner [14] analyzed vulnerabilities in NFC enabled smart phones. He developed a NDEF security toolkit to test the target NFC smart phone. His observation was NFC Data Exchange Format (NDEF) could be easily manipulated. He noticed that if the message sent by a smart poster is inserted with consecutive white spaces the user is unable to verify the security information displayed on the screen. And there is a weakness in the NDEF fuzzing process that if the value for the length of the payload field is set as two specific value, the phone will crash. After four crashes in a row, the phone automatically powered down. Another dangerous feature of the NFC enabled smart phone is that only the last 10 characters of the hostname is shown in the screen, which could fool the user into believing they are visiting the desired website while the phone is loading another malicious site.

NFC technology itself does not incorporate security mechanism to protect its framework and platform android operating system, for running NFC applications are weak to malware amongst OS [6]. Leakage of privacy happens in situation such as a Google NFC device user finishes grocery shopping using Google Wallet. [6] and [4] state that malicious software could plant itself without the user's knowledge and access SE to gain security information. Another work in [15] investigates the security of NFC in mobile payment system where the NFC

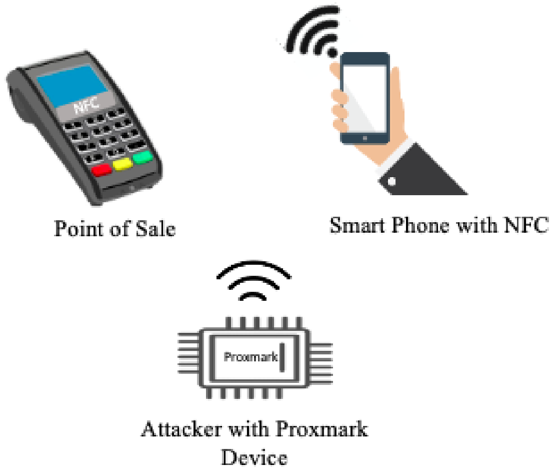

Fig. 1. Eavesdropping Attack

tag could contains malicious threats to redirect users to install e.g., malicious code without users knowledge.

III. Analysis of NFC Security Issues

NFC isn't secure as it looks. In this section, a possible NFC related attacks and their countermeasures are surveyed. Each attack will be explained using illustrative example, and then suggested countermeasures will be introduced to mitigate the risks of these attacks. At the end of this section, an evaluation of these attacks and countermeasures based on several factors such as cost of the attack and countermeasure and practicality of the attack and countermeasure are provided.

1) Eavesdropping: One common attack on wireless communications is eavesdropping attack, and Unfortunately, NFC technology is not secure against this attack [6].

The limited communication range of NFC devices which is few centimeters (about 10 cm) doesn't prevent the risk of eavesdropping attack completely. Any attacker with sufficient equipments can listen to the communication between two NFC devices. The main issue is how close an attacker needs to be able to conduct eavesdropping attack against NFC devices. In fact, this depends on the equipments of attacker such as antennas used, receiver used, and the environment of the attack such as noise, emitted signal. Other important factors such as the location of the attacker and position, the location of NFC device affect the attack operation. In addition, the communication mode affects the attack since there is a difference between listening to a NFC device in passive or active mode [9]. It is more difficult to listen to a NFC device in a passive mode because the target device may draw its source power from the electromagnetic field that is generated by the active device. According to [10] eavesdropping attack can be conducted up to a distance of 10m, when a NFC device is sending data in active mode, whereas this distance is significantly decreased to about 1m when the sending device is in passive mode.

Fig. 1 illustrates how an attacker that is closed to NFC environment can listen to the communication between two NFC devices. An attacker with sufficient knowledge and equipment such as Proxmark is capable of capturing NFC communication. Proxmark is an open source and powerful device currently available for researching RFID and Near Field Communication systems. Proxmark has the feature to snoop NFC traffic between a reader and tag it costs less than $500, more information about Proxmark can be found here [16].

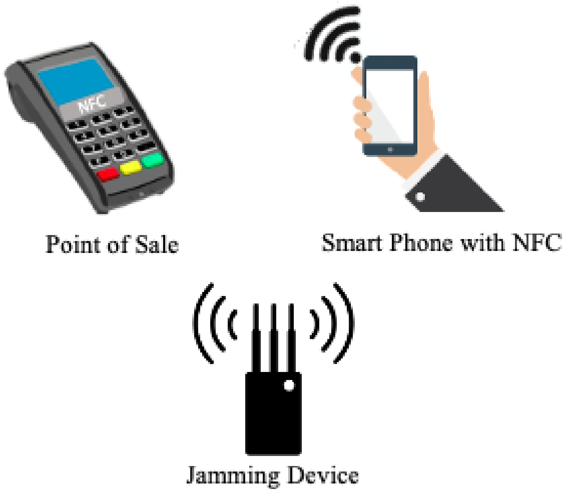

Fig. 2. Jamming Attack

Establishing a secure connection and using standard encryption algorithms between two NFC devices can protect against eavesdropping attack. A standard key agreement protocol such as RSA or Elliptic Curves could be used to establish a shared secret key between two NFC devices. The secret key then can be used to encrypt the communication using symmetric key algorithm such as AES or 3DES [10]. This countermeasure will ensure the confidentiality in NFC communication and will protect against eavesdropping attack.

2) Denial of Service: Wireless communication can be very vulnerable to Denial of service attacks or as knows Dos attacks. The results of Denial of service attacks can be anything from degradation of the wireless communication to a complete loss of availability wireless service. By launching a Denial of service attack, a malicious attacker can attempt to make a NFC deceive or a reader unavailable to its intended users. In this section, several Denial of service attack scenarios has been discussed.

One scenario of denial of service attack is by using a jamming device that target NFC environment [10]. The goal of jamming is to disrupt communications between two NFC devices.

Fig. 2 shows a malicious attacker with jamming device such as RFID jammer transmit a signal that interfere with the transmission between a mobile NFC phone and a reader of a service provider. This interference can destroy the transmitted data and cause denial of service. Almost there is no way to prevent jamming; however, there is a solution to deals with this scenario by continuously trying to detect jamming attack.

The solution is to let NFC devices check the radio frequency field while transmitting. This means the sending device could continuously check for such an attack scenario and could stop the data transmission when someone tries to jam the transmission.

Another Denial of service attack has been explained by [14], where the goal of the attack is to destroy trust relationship between customers and the service provider.

The following steps explain the scenario of this attack.

- A malicious attacker or a malicious competitor creates a tag that causes an NFC mobile phone to crash after scanning.
- The malicious attacker will sneak to the victim or the service provider and place the malicious tag on top of service provider tag.
- Any customer visit the victim or the service provider to get a service using NFC mobile phone will crash after scanning.
- The malicious tag cannot be linked to phone crash accident since it looks just like a normal tag, and this incident can destroy trust relationship between customers and the service provider

There is no solution for this attack; however, it can be detected using some tools such as fuzzing. More detail about this tool can be found in [14].

Another scenario of denial of service attack can be launched using empty NFC tag. Riyazuddin [7] indicated that just touching an NFC device with an empty tag causes a reaction of the device. The device will generate and an error message which is an easy way to occupy the device and make it unavailable. Adding a mechanism of controlling the NFC device such as NFC switch can help to prevent this attack scenario. The drawback of this solution is that the user has to turn on and off the NFC functionality each time when he needs to scan.

3) Phishing: Phishing attack is the act of attempting to obtain sensitive information such as passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication. Phishing attacks could easily be performed against NFC environment by modifying or replacing NFC tags.

The following steps and Fig. 3 explains how a malicious attacker can harvest sensitive information such as credit card information by launching a phishing attack against parking meter that uses NFC technology for completing the process of payment [8]:

- The attacker first create a malicious tag that contains false information such as the URL link that directs to a phishing site.
- The attacker will find a parking meter that uses NFC technology and replace the original tag at the parking meter with the malicious tag.
- In order to pay the meter fee, a victim with NFC mobile device such as Samsung phone scans the park meter tag in order to pay the required fee.
- The user will be asked to install a malicious app com.porkmobile which is basically a Web view to the phishing site.
- The user will enter sensitive information such as credit card information using the installed malicious app, and the attacker will collect these sensitive information.

There are several countermeasures can be used to prevent or mitigate phishing attack risk. One crucial factor of conducting phishing attack is to deceive the users by masquerading as a trustworthy entity, however; people who are aware about this phishing attack are difficult to deceive. User awareness and education about phishing attack is an important countermeasure since it helps to minimize the number of successful attacks. Cautious users will recognize the process of requiring installing new application with suspicious name and will investigate more about the name and originality of the application.

Gerald et. al. [5] suggests using signatures on tags and transporters and they indicate that would be suitable way to overcome this issue. Furthermore, applications market for NFC mobile such as Google's market can play a crucial role to prvent malicious applications that are suspicious to phishing.

A. Data Insertion

Data insertion attack goal is to insert a message into exchanged data between two NFC devices, when the answering device takes time to answer the original device. The attack can be launched only if the device has some delay that makes an attacker is able to transmit its message before the answering device. If both the attacker and the answering device transmit the data at the same time, the data will be overlapped and corrupted.

Data insertion attack can be launched between two NFC devices. The following scenario explains the attack steps:

- The attacker will place his malicious reader near the original reader device.
- The victim user will use the mobile NFC phone to transmit the data to the reader device.
- The malicious reader will reply directly to the victim user before the original reader.
- The original reader will reply to victim user after the attacker and the reply will be ignored by the victim's mobile NFC phone.

In order to prevent the data insertion attack between two NFC devices, there are three countermeasures can be employed. Firstly, the answering device should answer the original device with no delay. In this way the attacker would not be able to insert a message into the exchanged data between two NFC devices, because attacker can't be faster than answering device. Secondly, the answering device should listen to the channel while transmitting the data, so the device can detect any potential attack. Thirdly, establishing a secure channel between two NFC devices is the best approach to prevent any attack [10].

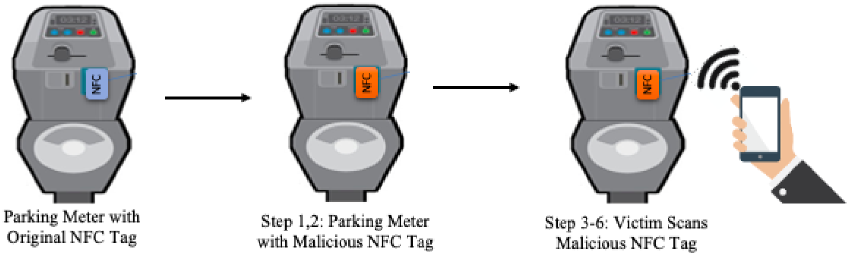
NFC
Parking Meter with Original NFC Tag
Step 1,2: Parking Meter with Malicious NFC Tag
Step 3-6: Victim Scans Malicious NFC Tag

Fig. 3. Phishing Attack Targeting at Parking Meter

B. Data Modification

Data modification is different than data insertion where attacker inserts a message into the exchanged data between two NFC devices. In data modification, the attacker can modify the exchanged data between NFC devices, so the receiving device will receive some valid but manipulated data. The feasibility of data modification attack relies on the amplitude of modulation [10]. It is difficult to launch data modification attack against NFC environment when the coding modulation is 100% in modified Miller coding modulation, this is because in 100% modulation the attacker is not able to alter a bit of value 0 to a bit of value 1. Although if a bit of value 1 is coming first (i.e. with a probability of 0.5), the attacker is able to alter a bit of value 1 to a bit of value 0. In 100% modulation, two half bits for radio frequency signal on and radio frequency signal off are checked by the decoder. The attacker should perform two steps to make decoder recognize one as zero and zero as one. First step which is a feasible step where attacker makes a pause in the modulation that loaded with carrier frequency. Second step which is practically impossible, where the attacker makes a pause of radio frequency signal that is received by the valid receiver. In this step, the attacker tries to overlap the original signal and the sending signal to make the receiver's antenna get a zero signal. However, it is easy to conduct the data modification attack when the modulation is 10% modulation. In 10% modulation, the decoder compares and assesses signal levels 82% and full. The attacker attempts to insert a signal to the 82% signal, in order to make the 82% signal become visible as a full signal and the actual full signal appears as 82% signal. Therefore, the valid bit of the reverse value of the bit would be decoded by the decoder. In conclusion, the attacker is feasible in all bits for 10% modulation, whereas is not feasible for all bits in 100% modulation.

Another example of data modification is exchanging electronic business cards or pairing information. Because there is no encryption or authentication in the transaction protocol, the means of security to ensure authenticity, integrity, and confidentiality should be implemented in the application layer.

A current common protocol, NFCIP-1, does not include the means of security. In this situation, the attackers can disturb the communication and modify the data. As shown in Fig. 4, if B disturbs the communication between A and C, and the communication does not include encryption or authentication. Thus, B can modify the exchanged data between A and C.

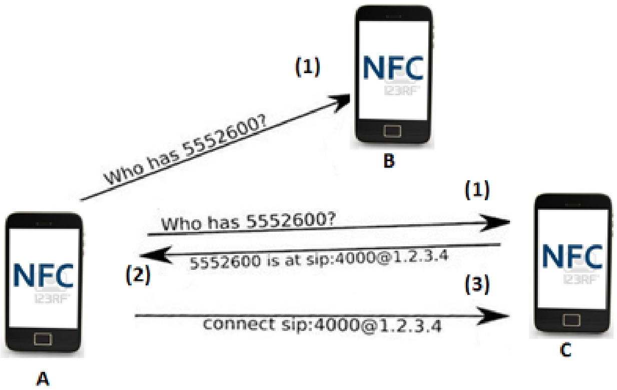

Fig. 4. Example of Data Modification over Peer Link.

There are several ways to protect against the data modification attack. First, the attacker would not be able to alter all the data transmitted by radio frequency link, if 106k baud in active mode has been used. It can be clearly seen that the active mode is important, however, this mode is vulnerable for eavesdropping attack. Furthermore, some bits in 106k baud can be modified. Second, the sending device checks constantly the radio frequency field while transmitting data to detect any potential attack. Third, establishing a secure connection between two NFC devices appears to be the best approach to protect against data modification attack [7].

C. Man In The Middle Attack

In Man in The Middle Attack (MITM), an attacker makes two parties believe that they are connecting to each other directly while in fact the whole conversation is directed by the attacker. In classical scenario, let assume Alice and Bob two parties want to talk to each other and Eve is the attacker who controls the entire conversation. Both parties Alice and Bob think they are receiving and sending data to each other whereas the whole data is coming from Eve.

Let's assume the same classic scenario but the link between the two parties Alice and Bob is an NFC link, where Alice would be in active mode and Bob uses passive mode. Alice wants to send data to Bob, so Alice generates the radio frequency field. The data can be eavesdropped by Eve, if Eve is closed enough, and actively disturbed the transmission to ensure the data hasn't been transmitted to Bob. In this situation, the attack can be detected by Alice through checking for any active disturbance. Alice would disconnect the communications [10].

Let's assume the protocol continue and is not been checked by Alice. Eve would generate radio frequency field to be able to send the data to Bob. But, this would cause two actively radio frequency fields. The first one is generated by Alice and the second one is generated by Eve. Bob would receive a data that is not understandable. As a result, this situation is practically impossible for man in the middle attacks to be conducted.

Another scenario, let us assume the same classic scenario, but this time the two parties Alice and Bob would be in active mode. Alice sends data to Bob, and Eve is able to eavesdrop the data. Eve disturbs the transmission to ensure that bob has not received the data. Again, if Alice has not checked for any active disturbance, the protocol would continue. Let us assume that the protocol continues. In active – active communication radio frequency field has been turned off by Alice, so Eve can send data to Bob. Eve turned on the radio frequency field and sends the data. In this situation, Alice expects an answer from Bob. As a result she would listen, and receive a data from Eve. Alice would detect a problem in the protocol, and disconnect the protocol. Consequently, it is impossible for Eve to send and receive a data from the two parities. In conclusion, in real world man in the middle attack practically is unfeasible to be conducted between two NFC devices [10].

As mentioned that man in the middle attack is practically impossible in NFC link. However, it is highly recommended to use active – passive communication mode. In addition, in order to detect any disturbance that launched by any attack, the active party should listen and check the radio frequency field during the transmission.

D. Data Corruption

The attacker needs a high power to be able to corrupt the data while transmitting between two NFC devices. However, this attack can be detectable, because the NFC devices can check the radio frequency filed during the data transmission and detect the type of attack. In addition, to perform data corruption attack the attacker requires more power than that can be detected by NFC device. Consequently, this attack can be detected by NFC devices [7].

E. Relay Attack

Relay attack is a type of man in the middle attack where the attacker attempts to manipulate the communication through relays the verbatim messages between two devices. Relay attack can be performing only if at least one of the attack devices supports card emulation. There are many possible scenarios to perform this attack.

The first scenario is when NFC is always on in smart phone, even if the phone not in use. A smart phone with payment application can make a transaction easily. As a result, this makes the phone vulnerable for relay attack. In this scenario, there are two attackers that are connected to each other through the Internet. The first attack has a proxy device and the second attack has a relay device with two NFC enabled devices or smart phones. In a public place such as public transportation where many people gather waiting for bus or metro to arrive. The attacker with rely device can get close to the victim's smart phone. Then, the proxy device performs NFC payment at payment station. The connection between the payment station and the victim's smart phone relays on the two devices. Francis et al. described the relay attack in NFC environment as shown in Fig. 5 [17].

The second scenario can be performed in modern smart phone where there are some privileges (known as jail breaking or rooting) that give you a full control over the smart phone. But, it also loses some security features of the smart phone, such as the application sandbox. In addition, the security features protect the secure elements where the NFC payment application resides. Thus, on a rooted smart phone, the secure elements are vulnerable more. In this scenario, the attacker attempts to let the user install a malicious application. The victim believes that he got the application access rights for the feature. Then, the malicious application would get the access right to execute the features. In the meantime the application gets an access to the secure elements, and informs the attacker over the Internet. Now, the attacker is able to make a payment by the victim's payment details [17].

To protect against relay attack, the smart phone's user should ensure that NFC in the smart phone is always off. In addition, the smart phone's user should preserve the security features to detect any malicious activity in any installed application.

F. Skimming Attack

There are two modes of secure element — external mode and internal mode.

1) External Mode: To emulate a tag, it requires smart card chips in NFC devices. In external mode, an external reader accesses the secure element and cannot distinguish between a smart card and an NFC device with a secure element. For example, there is a credit card applet in the secure element that turns the NFC handset into a mobile payment device.

2) Internal Mode: In internal mode, the host controller accesses the secure element (reading and altering). The running applications on the host controller of the handset can alter the information in the secure element. Hence, the users can remotely manage the information in the secure element by online connection (GPRS, Wi-Fi and etc.), also known as Over The Air (OTA) management. For example, when users use NFC for ticketing, ordinary smart card is a good choice. The tickets or money can be stored in the secure element remotely online.

In secure element, an index of applications is provided by both memory cards (NXP's Mifare Application Directory e.g.) and processor cards (JCOP e.g.). Therefore, it is vulnerable to a third party players because other applications in secure elements are exposed. The problem exists not only in NFC technology but also in other smart card industry.

G. Spoofing Attack

There is an unique ID for each contactless smart card chip (ISO14443 A: UID, ISO14443 B: PUPI, Felica: IDm). The length of them are 4, 7 or 10 Bytes. When collision happens

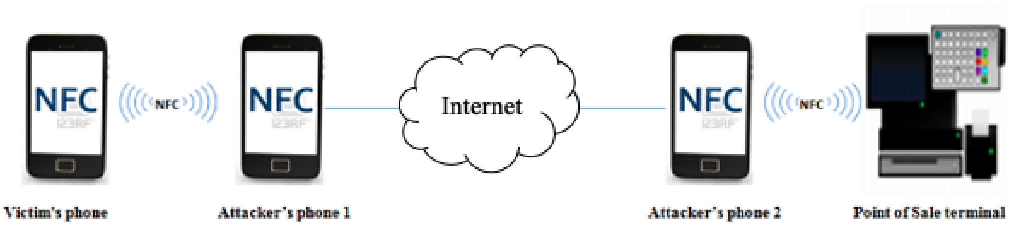

Fig. 5. NFC Relay Attack.

during the reading process, the unique ID is needed to prevent it by identification. The ID can be already acquired during the selection process of the transponder. The reading process does not include encryption or authentication of the reading device.

To prevent the collision, the unique ID is specified in the standard. A simple hardware like OpenPICC [18] can spoof someone's identity by simulating an ID. Therefore, if an application uses a fixed unique ID, it is easy to leak the holder's privacy. Because the reading process of the transponder does not include encryption, it is easy to eaves dropping the communication between the reader and the smart card chip to get the fixed unique ID. To avoid this situation, the unique ID can be created randomly when colliding, which is already used for NFC targets and e-passports [19]. It prevents the users from being tracked. However, it does not valid when victim is carrying an RFID transponder (a smart card or an NFC device).

H. Attacks and Countermeasures Evaluation

In this section, an evaluation and analysis between the surveyed attacks and their countermeasure is introduced. The evaluation is performed based on four factors which are attack cost, attack practicality, countermeasure cost and countermeasure practicality. The main goal of this evaluation and analysis is to evaluate and differentiate at the same time between mentioned attacks and countermeasures.

Attack cost describes the needed cost to perform an attack against near filed communication environment. The cost can be equipments such as jamming equipments or eavesdropping equipments, or the cost of the required time and effort to conduct the attack. Some attacks require purchasing extra equipments in order to launch the attack, for example, rely attack requires two NFC devices and proxy device and two involved attackers. On the other hand, there are several NFC related attacks that are not expensive and easy to launch such as denial of service attack.

Attack practicality is an important factor which describes the attacks quality of being practical, and the possibility of performing the attack. Not all NFC related attacks are practical; in fact some of the attacks are impossible to launch such as man in middle attack [10]. In addition, data modification attack is almost impossible for all bits in 100% modulation However; other attack such as eavesdropping, denial of service, phishing attack and rely attack are practical and can be launched with sufficient knowledge and equipment.

Countermeasures cost describes the needed cost to perform a countermeasure, such as extra resources or technical mechanisms. For some attacks such as denial of service attack the solution can be expensive since it requires hiring a security person or implementing a Closed-Circuit Television (CCTV) cameras system to monitor and prevent the access to the reader. However, other attacks such as relay attack require cheaper technical countermeasure such as turning off the NFC in the smart phone.

Another important factor is countermeasures practicality which describes the countermeasures quality of being practical, and the possibility of being performed. Some surveyed countermeasures are not practical to implement, for example, one of the data modification countermeasures is to use 106 K baud in active mode which will make NFC devices vulnerable to eavesdropping attack [7]. On the other hand, other suggested countermeasures are practical and very useful to implement such as establishing secure connection between NFC devices. Establishing a secure connection is very practical countermeasure and can be useful to prevent several NFC related attacks.

IV. Conclusions

Near filed communication is a promising technology and it is expected to be more integrated with future smart phones and to be an essential part of our daily lives. Master Card, Google and many payment services providers started to rely on near filed communication payment based technology which is anticipated to grow rapidly and broadly in the next few years. However; the security of near filed communication is still a concern and requires more deep analysis and further studies. This paper surveys many security threats, which are applicable to near filed communication, and covers countermeasures to protect against these threats. Near filed communication as technology cannot provide protection against many surveyed attacks such as eavesdropping or data modifications. Establishing a secure channel between NFC devices is a crucial mechanism to mitigate many security risks.

Future work of near filed communication could be how to design trustworthy operations of near field communication. Furthermore, other security related attacks should be more investigated such as NFC session hijacking, cloning attack, reply attack, and NFC skimming attack, which is reading an NFC device in a person's pocket. In addition, using near field communication in payment system impose many privacy issues which should be more studied and analyzed.

References

[1] A. N. Csapodi, Márton, "New applications for nfc devices," in *Mobile and Wireless Communications Summit*, 2007.

[2] F. Jeffrey, "The new paradigm for an interactive world [near-field communications]," *Communications Magazine, IEEE*, 2009.

[3] C. E. Ortiz, "An introduction to near-field communication and the contactless communication api," *http://goo.gl/icVkg*, 2008.

[4] M. Roland, "Practical attack scenarios on secure element-enabled mobile devices," in *International Workshop on Near Field Communications*, 2012.

[5] G. Madlmayr, J. Langer, C. Kantner, and J. Scharinger, "Nfc devices: Security and privacy," in *Availability, Reliability and Security*, 2008.

[6] S. H. Omkar Ghag, "A comprehensive study of google wallet as an nfc application," *International Journal of Computer Applications*, 2012.

[7] M. Riyazuddin, "Nfc: A review of the technology, applications and security." [Online]. Available: http://123seminarsonly.com/Seminar-Reports/023/46910687-Near-Field-Communications-Review.pdf

[8] I. Square, "Security risks of near field communication," *http://www.nearfieldcommunication.org/nfc-security-risks.html*, 2017.

[9] V. Damme, Gauthier, K. Wouters, and B. Preneel, "Practical experiences with nfc security on mobile phones," in *Workshop on RFID Security*, 2009.

[10] E. Haselsteiner and K. Breitfuß, "Security in near field communication (nfc)," 2006.

[11] S. Akter, S. Chellappan, T. Chakraborty, T. A. Khan, A. Rahman, and A. A. Al Islam, "Man-in-the-middle attack on contactless payment over nfc communications: Design, implementation, experiments and detection," *IEEE Transactions on Dependable and Secure Computing*, 2020.

[12] L. Francis, G. Hancke, K. Mayes, and K. Markantonakis, "Practical nfc peer-to-peer relay attack using mobile phones," in *RFIDSec*, 2010.

[13] E. H. et al., "Conditional privacy preserving security protocol for nfc applications," in *Consumer Electronics (ICCE), 2012 IEEE International Conference*, 2012.

[14] C. Mulliner, "Vulnerability analysis and attacks on nfc-enabled mobile phones," in *Availability, Reliability and Security*, 2009.

[15] M. Badra and R. B. Badra, "A lightweight security protocol for nfc-based mobile payments," *Procedia Computer Science*, vol. 83, pp. 705–711, 2016.

[16] "Proxmark3," *https://code.google.com/p/proxmark3/wiki/HomePage?tm=6*, 2007.

[17] R. Vermaas, "The security risks of mobile payment applications using near-field communication," 2013.

[18] "Openpcd http://www.openpcd.org/," 2007.

[19] I. Naumann, "Advanced security mechanisms for machine readable travel documents extended access," *Federal Office for Information Security, Tech. Rep.*, 2006.